UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/727,062	11/30/2000	Paul W. Dent	4015-721	2720

24112 7590 09/27/2005

COATS & BENNETT, PLLC
P O BOX 5
RALEIGH, NC 27602

EXAMINER
POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 09/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/727,062	**Applicant(s)** DENT, PAUL W.	
	Examiner Peter Poltorak	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 July 2005*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. The Amendment, and remarks therein, received on 07/05/05 have been entered and carefully considered.
2. The Amendment introduces new limitations into the original independent claims 1, 6, 11 and 19.

Response to Amendment

3. Applicant's arguments have been carefully considered but they were not found persuasive.
4. Applicant argues § 102 rejections pointing out that "NT password screen is not a password-protected secure function". Then applicant follows with various statements that are not understood.
5. It is not clear how applicant's argument relate to the rejections. For example, the examiner has never claimed that the NT password screen is not a password-protected secure function. As a result, applicant's arguments are addressed as best understood.
6. The secure function that a received command executes *(secure attention sequence SAS started by pressing CTRL-ALT-DEL)* is a request for a token that is received upon successful authentication. *(For simplicity one can consider a user authentication as the secure function.)* The received command results in displaying a password entry screen *(Hadfield et al, pg. 80-81, Logon process).*
7. The examiner also takes the opportunity to point out to applicant that his argument that "users do not need to enter a password to invoke screen to the user at logon" is

not reflected in the claim language, and points applicant to *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

8. Similarly, in response to arguments directed to *Ozzie's* teaching, the examiner points out that *Ozzie's* invention is directed towards a user authentication.

9. As a result, the previous rejections are maintained. However, for a more intuitive understanding of how applicant's invention relates to available prior art, an additional art rejection is provided.

10. Claims 1-22 have been examined.

Claim Rejections - 35 USC § 102

> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1- 4, 11 and 19 are rejected under 35 U.S.C. 102(b) as being anticipated by *Windows NT* as evidenced by *Ozzie et al. (Patent No. 5664099), NT Workstation Resource Kit (http://web.archive.org/web/20000306015737/http://is-it-true.org/nt/atips/atips71.shtml), Carter (Alan R. Carter,"Windows NT 4.0 MCSE Study Guide", 1997, ISBN: 0764530879), TechNet (http://www.mabuse.de/sources/Microsoft%20TechNet%20-%20Securing%20Your%20NT%20Network%20Starts%20With%20the%20Basics.htm)* and *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213).*

12. *Carter* teaches a password-protected secure function *(logon process)* wherein a user is prompted to enter a password by displaying a password entry screen *(logon*

information box, Carter pg. 389) and NT Workstation Resource Kit teaches the password entry screen displaying authentication indicia *(user name of the last person who logged on to the system, NT Workstation Resource Kit, § 1).*

13. *Carter* also teaches obtaining said password and indicia from a user and storing authentication indicia recognized by said user in said computing device in a security module *(SAM, Carter, pg.389)*, storing and saving current setting of a status table/alternate status table *(Carter, fig.21-9, pg.795)* in random access memory used by an operating system in said computing device, each entry in said status table relating to a currently saved (in memory) current executing program *(process)* and containing a status indication *(CPU, CPU time)* associated with said currently executing program *(Carter, fig.21-9, pg.795)* including the program needed by the security module *(winlogon, Carter, fig.21-9, pg.795 and TechNet). Hadfield et al.* teaches a computing device wherein the secure attention sequence (SAS: ALT+CTRL+DEL) displays the Windows NT operating system log-on screen *(Hadfield et al, pg. 80-81, Logon process).*

This reads on storing authentication indicia recognized by a user in a memory of the computing device and on receiving a command to execute a password-protected secure function, prompting the user to execute a password associated with the secure function by displaying a password entry screen containing the authentication indicia responsive to receiving the command.

14. *Hadfield et al.* teach that the system authenticates (using password) and issues a token upon successful authentication to the user *(Hadfield et al, pg. 80-81, Logon process).*

    This reads on executing the password-protected secure function based on the validity of the password entered by the user.

15. Password entry screens are removed upon successful entry of a password.

16. The publications do not explicitly teach removing said password entry screen from said display nor do they explicitly teach displaying said authentication indicia for a limited time. However, this feature is inherent as *Carter* shows on page 389 that in order to have password entry screen displayed a user action is required.

17. The security function is handled by a security module *(the Security Reference Monitor, Hadfiled et al., pg. 68).*

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. Claims 5-10 and 13-18 are rejected under 35 U.S.C. 103(a) as being obvious over *Windows NT* as evidenced by *Ozzie et al. (Patent No. 5664099), NT Workstation Resource Kit (http://web.archive.org/web/20000306015737/http://is-it-*

true.org/nt/atips/atips71.shtml), Carter (Alan R. Carter,"Windows NT 4.0 MCSE Study Guide", 1997, ISBN: 0764530879), TechNet (http://www.mabuse.de/sources/Microsoft%20TechNet%20-%20Securing%20Your%20NT%20Network%20Starts%20With%20the%20Basics.htm) and *Hadfield et al. (Lee Hadfield, Dave Hater, Dave Bixler, "Windows NT Server 4 Security Handbook", 1997, ISBN: 078971213).*

19. *Windows NT* teaches a computing device executing the password-protected secure function as discussed above.

20. As per claims 7-8, 13-16 inhibiting and operating system from responding to interrupts and as inhibiting context-switching by an operating system to programs not needed by the security module *(such as authentication module that uses the SAS)* would be implicit as *Hadfiled et al.* discloses that the intention of the SAS is to prevent spoofing *(Hadfield et al, pg. 81).*

21. As per claims 9 and 17 *Windows NT* does not teach changing status table settings to inhibit execution by said operating system of said programs not needed by said security module.

    The examiner takes Official Notice that control of programs through status table settings is old and well-established in the art. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to inhibit programs during login by switching status table for motivation of benefit of controlling programs in the execution of the security module

22. As per claims 10 and 18 *Windows NT* does not teach an alternate status table with entries relating to program needed by the security module.

    The examiner takes Official Notice that use control of programs through alternate status tables with entries relating to programs needed by security modules is old and well-established in the art. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use an alternate status table during execution the security module by the operating system for motivation of benefit of accessing programs needed in the execution.

1. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Carter* in view of *Zizzi (U.S. Patent No. 6185681).*
2. *Carter's* teaching in reference to the device comprising said secure processor and said memory has been discussed previously.
3. *Carter* does not teach the device comprising a smart card. Zizzi teaches the device comprising secure processor and memory *(Fig: 1)* and a smart card (*with a secure processor and memory*, *Zizzi, pg.2 lines 65-68)*; as it is obvious from *Fig. 1* that the device contains a card reader *(object 26)* in which card is inserted. *Zizzi* also teaches that smart cards used along with users' passwords enhance security *(Zizzi, pg.2 lines 65-68).*
4. It would have been obvious to one of ordinary skill in the art at the time the invention was made to improve the device containing said secure processor and said memory so that it would have comprised a smart card in Windows NT. One of ordinary skill

in the art would have been motivated to perform such a modification to increase security of the system utilizing Windows NT.

23. Claims 12, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Windows NT* as evidenced by *Ozzie et al. (Patent No. 5664099)*, *NT Workstation Resource Kit (http://web.archive.org/web/20000306015737/http://is-it-true.org/nt/atips/atips71.shtml)*, *Carter (Alan R. Carter,"Windows NT 4.0 MCSE Study Guide", 1997, ISBN: 0764530879)* and *TechNet (http://www.mabuse.de/sources/Microsoft%20TechNet%20-%20Securing%20Your%20NT%20Network%20Starts%20With%20the%20Basics.htm)* in view of *Smeets et al. (U.S. Patent No. 6769062)*.

24. *Windows NT* teach a secure processor and memory as discussed above.

25. *Windows NT* do not teach a removable security module comprising a smart card and containing the secure processor and the memory.

26. *Smeets et al.* teach a removable security module comprising a smart card that contains a secure processor and memory (*Smeets et al.,* col. 3 lines 35-48).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the secure processor and the memory as taught by *Windows NT* in the security module comprising a smart card as taught by *Smeets et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to minimize the threat of probing for the illicit purpose of extracting stored secret information.

27. Claims 12, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Windows NT* as evidenced by *Ozzie et al. (Patent No. 5664099)*, *NT Workstation Resource Kit (http://web.archive.org/web/20000306015737/http://is-it-true.org/nt/atips/atips71.shtml)*, *Carter (Alan R. Carter,"Windows NT 4.0 MCSE Study Guide", 1997, ISBN: 0764530879)* and *TechNet (http://www.mabuse.de/sources/Microsoft%20TechNet%20-%20Securing%20Your%20NT%20Network%20Starts%20With%20the%20Basics.htm)* in view of *Steinberg (U.S. Pub. No. 20030159042)*.

28. *Windows NT* do not teach a removable security module comprising a smart card and containing the secure processor and the memory.

29. Steinberg teaches a removable security module comprising a smart card that contains a secure processor and memory *(Steinberg, Abstract and [0017])*.

    It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the secure processor and the memory as taught by *Windows NT* in the security module comprising a smart card as taught by *Steinberg*. One of ordinary skill in the art would have been motivated to perform such a modification in order to customize the security module for a particular user.

---

30. Claims 1- 11 and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Panescu et al. (U.S. Patent No. 6106460)* in view of *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)*.

31. As per claim 1 *Panescu et al.* teach that "access to the operating system is restricted only to authorized service personnel, through executing the password protected SERVICE application" *(Panescu et al., col.11 lines 12-16).* Furthermore, *Panescu et al.,* teach that "the selection of the SERVICE push button control 132 runs the service application A7. The service application A7, when executed by the MPU 28, displays the service sub-window 516, as shown in FIG. 26." *(Panescu et al., col. 30 lines 20-23)* and that "the service window 516 displays a dialog box 518, which contains input fields for the operator to enter a SERVICE IDENTIFICATION 520 and a PASSWORD 530. When the OKAY button 532 is selected, the service application A7 accepts the inputs in the fields 520 and 530 and compares them to known identification and password codes embedded in the application A7. When the inputs match the known codes, the service application A7 terminates the GUI 46 and returns control of the MPU 28 to the underlying operating system 44. The service application A7 provides access to the underlying operating system 44 and associated host computer functions only to authorized service personnel." *(Panescu et al., col. 30 lines 28-39).*

32. This reads on receiving a command to execute a password-protected secure function, prompting the user to enter a password associated with the secure function by displaying a password entry screen responsive to receiving the command, and executing the password-protected secure function based on the validity of the password entered by the user

33. *Panescu et al.* do not teach a password entry screen containing the authentication indicia.

34. *Pfleeger* teaches authentication indicia during authentication process that involves password *(a display implementation of a display of some information known only by the user and the system, Impersonation of Login, Pfleeger, pg. 263-264).*
It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include the authentication indicia in a password entry screen. One of ordinary skill in the art would have been motivated to perform such a modification in order to ensure the authenticity of the authenticator.

35. Claims 11 and 19 are substantially equivalent to claim 1; therefore claims 11 and 19 are similarly rejected.

36. As per claims 5-6 *Pfleeger* teaches halting any running process in the processing terminal during an authentication process involving use of the password *(Pfleeger, Impersonation of Login, pg. 263).*
It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to halt programs running on the computing device while the password entry screen is displayed *(during authentication process)* for motivation of security benefit. Enabling programs necessary for inputting the password as well as restarting halted programs after the password entry screen is removed would be implicit.

37. As per claim 2 the very purpose of the indicia as taught by *Pfleeger* is to prevent spoofing or replay attacks and as a result it would have been obvious to one of

ordinary skill in the art at the time of applicant's invention to store the authentication indicia in a security module for motivation of protecting the indicia.

38. As per claim 3 *Panescu et al.* in view of *Pfleeger* do not explicitly teach that the password entry screen is displayed for a limited time.

Official Notice is taken that it is old and well-known practice to limit time of displaying password entry screen such as Microsoft Windows Logon Window for motivation of benefit of minimizing the time that the system is in a protective mode. The examiner considers that the Microsoft Windows Logon Window is comparable to displaying password entry screen.

39. As per claim 4 not only the indicia as taught by *Pfleeger (information displayed to a user)* are based on the user input but also it is old and well-known to receive input from a user, such as username and later to display the name of the last person who logged on to the system in the authentication window, such as Microsoft Windows logon screen *(e.g. NT Workstation Resource Kit, § 1).* The examiner considers that receiving user's name from a user and later displaying the name of the user in an authentication window is comparable to displaying the authentication indicia obtained from the user.

40. As per claims 9 and 17 *Panescu et al.* in view of *Pfleeger* do not teach changing status table settings to inhibit execution by said operating system of said programs not needed by said security module.

The examiner takes Official Notice that control of programs through status table settings is old and well-established in the art. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to inhibit programs during login by switching status table for motivation of benefit of controlling programs in the execution of the security module

41. As per claims 10 and 18 *Panescu et al.* in view of *Pfleeger* do not teach an alternate status table with entries relating to program needed by the security module.

42. The examiner takes Official Notice that use control of programs through alternate status tables with entries relating to programs needed by security modules is old and well-established in the art. Thus it would have been obvious to one of ordinary skill in the art at the time the invention was made to use an alternate status table during execution the security module by the operating system for motivation of benefit of accessing programs needed in the execution.

43. Claims 12 and 20-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Panescu et al. (U.S. Patent No. 6106460)* in view of *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* and in further view of *Zizzi (U.S. Patent No. 6185681).*

44. *Panescu et al.* in view of *Pfleeger* teach a device comprising a secure processor and memory as has been discussed previously.

45. *Panescu et al.* in view of *Pfleeger* do not teach the device comprising a smart card.

46. Zizzi teaches the device comprising a secure processor and memory *(Fig. 1)* and a smart card (*with a secure processor and memory*, *Zizzi, pg.2 lines 65-68)*; as it is obvious from *Fig. 1* that the device contains a card reader *(object 26)* in which a card

is inserted. *Zizzi* also teaches that smart cards used along with users' passwords enhance security *(Zizzi, pg.2 lines 65-68).*

It would have been obvious to one of ordinary skill in the art at the time the invention was made to improve the device containing said secure processor and said memory so that it would have comprised a smart card. One of ordinary skill in the art would have been motivated to perform such a modification to increase the system's security.

47. Claims 12, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Panescu et al. (U.S. Patent No. 6106460)* in view of *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* and in further view of *Smeets et al. (U.S. Patent No. 6769062).*

48. *Panescu et al.* in view of *Pfleeger* teach a secure processor and memory as discussed above.

49. *Panescu et al.* in view of *Pfleeger* do not teach a removable security module comprising a smart card and containing the secure processor and the memory.

50. *Smeets et al.* teach a removable security module comprising a smart card that contains a secure processor and memory (*Smeets et al.*, col. 3 lines 35-48).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the secure processor and the memory in the security module comprising a smart card as taught by *Smeets et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to minimize the threat of probing for the illicit purpose of extracting stored secret information.

51. Claims 12, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Panescu et al. (U.S. Patent No. 6106460)* in view of *Pfleeger (Charles P. Pfleeger, "Security in computing", 2nd edition, 1996, ISBN: 0133374866)* and in further view of *Steinberg (U.S. Pub. No. 20030159042)*.

52. *Panescu et al.* in view of *Pfleeger* do not teach a removable security module comprising a smart card and containing the secure processor and the memory.

53. Steinberg teaches a removable security module comprising a smart card that contains a secure processor and memory *(Steinberg, Abstract and [0017])*.
It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to implement the secure processor and the security module comprising a smart card as taught by *Steinberg*. One of ordinary skill in the art would have been motivated to perform such a modification in order to customize the security module for a particular user.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, THIS ACTION IS MADE FINAL. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at (866) 217-9197 (toll-free).

9/10/05

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100